



## Podcast Transcript

# CA Privacy Law Reboot CCPA 2.0

**Date:** August 26 2020

**Guest:** Alan Friel, **Host:** Amy Kattman

**Run Time:** 19:12

**For questions and comments, contact:**



### Alan Friel

Partner

Los Angeles

T: +1.310.442.8860 | [afriel@bakerlaw.com](mailto:afriel@bakerlaw.com)

---

**Kattman:** The California Consumer Privacy Act of 2018, or CCPA, last amended in 2019, forever changed the consumer privacy compliance landscape in the U.S. by applying European-inspired privacy principles but reworking them in a uniquely American way. To make things even more interesting, looming on the November horizon is CCPA 2.0, or the California Privacy Rights Act, CPRA. I'm Amy Kattman, and you're listening to BakerHosts.

On today's episode, we will discuss both the CCPA and the upcoming CPRA, which will appear on California's November ballot. Our guest today is Alan Friel, a partner in BakerHostetler's Digital Assets and Data Management Practice Group and leader of the Consumer Privacy team. Welcome to the show, Alan.

**Friel:** Hi.

**Kattman:** So Alan, we had the CCPA, which has been in effect less than a year, and now, on the Nov. 3 ballot, there's going to be the CPRA. Could you provide a brief background on the CCPA and where things stand so far?

**Friel:** Sure. The California Consumer Privacy Act, or CCPA, is a paradigm-changing consumer privacy law that was inspired by privacy regimes in Europe and other parts of the world, and [it] has resulted in most U.S. consumer-facing businesses having had to map their data practices, disclose those practices in published pre-collection and enterprisewide notices, and be able to honor consumer requests to access [and] obtain consumer-specific information on how their PI, or personal information, that is, is collected, used and shared; receive a transportable copy of their PI; delete their PI subject to limited retention exemptions; and restrict the sale of their personal information.

The CCPA went into effect on Jan. 1 of this year, with a one-year delay in the application to business-to-business communications and human resources data, excepting for the private right of action for failure to maintain reasonable security and a pre-collection notice for human resources.

Kattman: I understand that the regulations were not ready in January. What is the status of that?

Friel: Enforcement by the attorney general was delayed until July 1, while the attorney general developed regulations that provide guidance on the meaning of the act and how businesses need to comply. That gave industry a little breathing room to perfect their compliance with the act. That date is obviously now past, and in early July the AG commenced multiple investigations of businesses, with reportedly an emphasis on how the so-called Do Not Sell right was being addressed. The AG also promulgated final regulations in June. Those, while published, have not gone into effect, as they remain under review by the Office of Administrative Law. However, there's no reason to think they will not become fully effective as published by the deadline at the end of this month. Businesses should be assessing their compliance programs in light of those regs and the Statement of Reasons and Responses to Public Comments that accompany them.

Kattman: What kind of ongoing obligations do companies have?

Friel: In addition, companies will need to update their California privacy notice to reflect 2020 practices before Jan. 1 of next year, and companies that process personal information of 10 million or more consumers this year will have robust reporting obligations on their consumer rights request responses from this year, which must be published by July 1 of next year. But wait, just when you thought you had it all figured out, [the] CCPA is up for a complete overhaul in the form of the California Privacy Rights Act, or CPRA, a ballot measure which proposes to create new consumer rights and business obligations.

Kattman: So Alan, you've given us a nice background on [the] CCPA. How did the CPRA come into play, and really, how is it different [from] the CCPA?

Friel: To understand [the] CPRA, you have to look back at the genesis of [the] CCPA. Back in 2018, a consumer privacy advocate named Alastair Mactaggart and his Californians for Consumer Privacy organization developed a ballot initiative that was the forerunner of the CCPA. One key pain point for industry and policymakers was that it would have created a broad private right of action for any violation of the law. Ultimately, a legislative compromise was worked out, with a more limited private right of action restricted to security incidents attributable to failure to maintain reasonable security, and all other enforcement was vested solely in the attorney general.

That law was passed, and the ballot measure was withdrawn literally on the eve of printing the ballots. The result is the CCPA that is now in effect. The original ballot measure proponents have, however, been disappointed with certain

aspects of the rollout and interpretation of the CCPA, particularly regarding the interpretation of the definition of “sale” and the scope of the opt-out that relates to digital advertising, and have proposed a comprehensive set of what they see as refinements, clarifications and enhancements in the form of the CPRA, a ballot measure that would amend the CCPA. [A total of] 623,212 signatures were required for the CPRA to appear on the fall ballot on Nov. 3, and approximately 900,000 were submitted. The measure has been certified.

Kattman: What exactly will Californians be voting on?

Friel: The California secretary of state recently published a ballot title and summary for the CPRA, now known as Prop. 24. The title is “Amends Consumer Privacy Laws.” The summary states the measure as follows: Permits consumers to (1) prevent businesses from sharing personal information, (2) correct inaccurate personal information, and (3) limit businesses’ use of sensitive personal information; prohibits businesses’ retention of personal information for longer than is reasonably necessary; triples maximum penalties for violations concerning consumers under the age of 16; and establishes the California Privacy Protection Agency to enforce and implement the law and impose administrative fines. So, accordingly, it sounds fairly innocuous and probably attractive to many voters. In fact, it’s polling in the mid-80 percent [range]. The impact on industry, however, will be material.

Kattman: Alan, you mention impact. What will be the impact of the CPRA on digital advertising?

Friel: This is an issue that seems to have most driven the proponents to seek to amend the existing law. The concept of “sale” under [the] CCPA is somewhat ambiguous, and the regulations do not resolve the controversy of what types of commercial disclosures that lack an exchange of cash consideration qualify as a sale that is subject to the CCPA’s consumer opt-out. The CPRA expands the Do Not Sell opt-out to include sharing of personal information or cross-contextual behavioral advertising, regardless of the exchange of monetary consideration. An opt-out right is also provided for precise location-aware advertising. Notice of opt-outs must be passed down by the business to the [data’s] recipients, who are then required to also honor the opt-out – provided, however, the business is not responsible for the recipients’ failure to do so.

“Cross-contextual behavioral advertising” is defined to mean the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses’ distinctly branded websites, applications or services other than the businesses’ distinctly branded website, application or service with which the consumer intentionally interacts. This is what is known as interest-based or behavioral advertising, which depends upon the building of psychographic and/or demographic profiles on us to enable advertisers to send us more relevant ads. That’s why, for instance, I may get ads on fly fishing but you may get them on running shoes.

Kattman: I understand the CPRA will regulate sensitive information about consumers. Can you explain that?

Friel: The CPRA would require definitive opt-out of that kind of data sharing. However, what it does not answer is the question of at what point. The ad and publishing industries have been split as to whether publishers are making service data available to ad tech or if ad tech is independently collecting the information. That question will remain unsolved by the initiative, but [the] CPRA makes clear that the multiple downstream disclosures inherent in intraspace advertising are subject to opt-out unless restricted to limited use, such as to provide certain permitted services to the data controller, a use case far more narrow than what happens in the intraspace advertising ecosystem.

[The] CPRA also requires, at or prior to the collection of sensitive personal information, notice by category of the purposes of collection and use of that data, and if it is sold or shared, along with notice of the ability to opt out of the sharing or sale, or any other use not reasonably necessary to enable the business to provide the consumer with requested goods or services. This will require a homepage link to an opt-out entitled Limit the Use of My Sensitive Information. So this affects certain demographic targeting. More specifically, sensitive personal information includes such data as consumers' financial information, precise geolocation, religious or philosophical beliefs, union membership, the contents of a consumer's communication, [and] genetic data or other health information. Notably, however, sensitive PI that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this new consumer right and would be treated as regular PI. Accordingly, consumers' rights are limited to a business's use and disclosure and would not apply to sensitive PI that is not used to generate consumer inferences, in other words, [for] advertising purposes.

Kattman: So, talking more about businesses, how will they need to revise their CCPA compliance program[s] to meet the requirements of this new law?

Friel: [The] CPRA increases the potential repercussions for noncompliance and removes an obligation that the government give notice and a 30-day opportunity to cure noncompliance – provided, however, that the new enforcement agency created by Prop. 24 will have the discretion to permit a one-time cure. That new agency will have authority to bring administrative enforcement actions and levy fines and will be well funded. Penalties for violations involving children are increased. However, the CCPA's limited private right of action will not be expanded.

The ballot measure's changes to the CCPA affect more than just digital advertising. It limits ancillary uses of personal information even if disclosed at the time of collection unless reasonably necessary and proportionate to the primary purpose. For instance, it might be argued that a publisher's selling of personal information to unrelated third parties [that was] obtained when a consumer registers for or uses a website or mobile app, for instance a live weather app, even if disclosed prior to collection and notwithstanding the right to opt out of

sale, is not reasonably necessary to provide the services. In the example I gave, how hot it is in Palm Springs – 118 degrees at the moment, if you're interested – and in the case of paid subscription services, [the PI is] not proportionate to obtain those services.

Kattman: Beyond the limitations of what companies can do with consumer data, how else will [the] CPRA regulate businesses?

Friel: [The] CPRA will send businesses back to further redraft their commercial agreements. It requires detailed written contracts limiting use and obtaining other commitments and providing for remediation rights, not just from service providers and contractors, but from recipients in a sale or cross-context behavioral advertising sharing. The result: necessitating updates to vendor agreements beyond what was done for [the] CCPA, in addition to requiring new forms of recipient agreements for sharing and sales. The ballot measure limits retention of personal information to only so long as required to meet the collection and use purposes stated at or prior to the time of collection, and requires businesses to state the retention period or methods of determining it as part of the pre-collection notice.

Kattman: Alan, companies have been struggling with the CCPA's deletion right. Does the CPRA address that at all?

Friel: The CPRA modifies the deletion request process. The CCPA requirement that a business that receives a deletion request direct its service providers to delete the data is changed to an obligation to notify them of the deletion request. [The service providers] are then, in turn, obligated to cooperate with the business and delete the personal information if further directed to do so, except to the extent they have their own retention right under the act.

Service providers and contractors have the obligation to pass this notification down to their subcontractors. Further, a business's deletion request notification requirement is expanded also to third parties to which the business sold or shared personal information unless this proves impossible or involves a disproportionate effort.

Kattman: Are there other consumer rights addressed by [the] CPRA?

Friel: The CPRA would also codify privacy by design. It contemplates regulations to require businesses that are involved in processing of personal information that creates a significant risk to privacy or security to conduct privacy risk assessments and to perform annual security audits. The CPRA expands existing consumer rights. Personal information collected after Jan. 1, 2022, shall not be subject to the current limitation of a one-year lookback for consumer rights to know, except to the extent responding with regard to older data would be impossible or involve a disproportionate effort. Further, [the] CPRA creates an additional consumer right: the right of correction to change or update your personal information.

Kattman: Alan, now let's talk about timing. When will the different provisions of the new law go into effect?

Friel: As I said, the CPRA will be on the November ballot, and it's polling in the 80-plus percentile. If approved by a majority vote this fall, the CPRA would become operative shortly after the election, but most of the new obligations on businesses would not become operative until Jan. 1, 2023, and would not be enforceable until July 1, 2023. However, the state would be obligated to promulgate related regulations by July 1, 2022, and the data that would be subject to the CPRA's new requirements would be personal information collected after Jan. 1, 2022. One aspect of the CPRA which would take immediate effect is the two-year extension of the statutory exclusions of HR and B2B communications data, which are currently set to sunset at midnight on Dec. 31 of this year.

Kattman: Wow, that is a lot of information to take in. Could you summarize it for us, Alan?

Friel: In conclusion, less than a year into the effectiveness of the CCPA, it seems likely that the scope of consumer rights and business obligations is about to be significantly expanded. While many will appreciate the additional two-year extension of the B2B and HR carveouts for most consumer rights, businesses that are only just wrapping their hands around how to comply with the CCPA may find themselves spending 2021 preparing for additional obligations. Not to worry, however. The work you've done in developing a CCPA-compliant information governance program should enable you to prepare for the new law by merely refining that existing program. In other words, most companies have already done the heavy lifting, and we're here to help you apply CCPA 2.0 to your existing compliance program.

Kattman: Thank you, Alan. If you have any questions for Alan, his contact information is in the show notes. As always, thanks for listening to BakerHosts.

Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practice and experience, please visit [bakerlaw.com](http://bakerlaw.com).